ISO/IEC JTC 1/SC 27 N 2461

ISO/IEC JTC 1/SC 27/WG 3 N 484

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN

DOC TYPE:	Expert Contribution
TITLE:	German expert contribution on "Use of suppliers' declaration of conformity for IT security products"
SOURCE:	German expert (J. Appel)
DATE:	1999-10-04
PROJECT:	
STATUS:	This document was available at the 19th SC 27/WG 3 meeting in Columbia, USA, October 4-8, 1999. It is being circulated within SC 27 for information.
ACTION ID:	FYI
DUE DATE:	
DISTRIBUTION:	P, O, L Members W. Fumy, SC 27 Chairman M. De Soete, T. Humphreys, M. Ohlin, WG-Conveners
MEDIUM:	Server
NO. OF PAGES:	12

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile:+ 49 30 2601-1723; E-mail: passia@ni.din.de
HTTP://www.din.de/ni/sc27

ISO - International Organisation for Standardisation
IEC - International Electrotechnical Commission

JTC 1 - "Information Technology"
SC 27 - "Security Techniques"
WG 3 - "Security Evaluation Criteria"

TITLE: Use of Suppliers' Declaration of Conformity for IT Products

SOURCE: Johannes Appel, Germany

DATE: 1999-10-04

PROJECT:

STATUS: For consideration at the 19 th SC 27/WG 3 meeting in Columbia, MD, U.S.A., October 4 - 8, 1999.

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile:+ 49 30 2601-1723; E-mail: passia@ni.din.de
HTTP://www.din.de/ni/sc27

Content

TBD

Preface

The Information Technology (IT) is a decisive factor of our live in today society. E-Business, E-Mail, and World Wide Web are progressing in an unprecedented pace. This has increased the interest of public and institutional customers in the security functionality and evaluation of IT products. The key questions are: At what level of security do I have to operate my IT products to secure my business? Can I trust that the security functionality, its effective and correctly implemented? This has stimulated growing interest in the different methods to prove the trustworthiness and quality of IT products.
Developer and manufacturer conducts already extensive simulations, design reviews, tests and evaluations during the development and manufacturing as part of their quality management. In order to gain additional evidence about the quality and the effectiveness of the security functionality of an IT product the manufacturer or distributor can call on an independent party. This is normally a so-called Third Party like a Consultant, Test Laboratory, Certification Agency. The consultation or evaluation through an independent party leads in general to an increase in trustworthiness. Critics claim that the drawback of this method are manifold:

- risk of disclosure of newly developed designs
- risk of outflow of know-how
- increase in development cycle and time-to-market
- increase in product costs

Because of rapidly decreasing of the time-to market and increasing competition the IT industry is searching for efficient alternatives for simulation, testing, evaluation and certifying of their products. The IT market needs are based on scalable security. Simple authentication and integrity checks of communication and stored date require a different security level and trustworthiness than the handling of medical data or a legal act attested by a notary. It should be up to the public or institutional consumer to select an IT product based on his need for security and trustworthiness. The will give the manufacturer the freedom of choice which evaluation criteria, testing and evaluation method as well as certification alternative he is going to apply to meet the final customer needs. The consumer on the other hand can choose the product which best fits his needs to minimise his security risk.

Scope

This technical report formalises the Manufacturer commitment to his product with a Suppliers‘ Declaration of Conformity (SDoC). It describes the available alternative methods to demonstrate that a product meets the security and further quality requirements. The technical report concentrate on the aspect which will help to establish trust in connection with the development, manufacturing, and distributor in particular during testing, evaluation, and certification of the security relevant functions. The main focus is on the use of the SDoC. The required structure and content of the SDoC for IT security products is given. It is intent is to increase the transparency and comparability for the final consumer in selecting trustworthy products.

A documented sample declarations in Annex A may serve as guidance for a proper application of this Technical Report.

Reference

ISO Standards

ISO/IEC 15408-1,-2,-3	Evaluation Criteria for IT Security
ISO/IEC Guide 22	Information on Manufacturer's Declaration of Conformity with standards
Guide 25	General criteria for suppliers declaration of conformance or other technical specifications
ISO 12119	Information Technology Software Products – Quality requirements and evaluation

CEN/CENELEC

EN 45001	General criteria for the operation of testing laboratories
EN 45013	General criteria for certification bodies operating certification of personnel
EN 45014	General criteria for suppliers declaration of conformance

European Union (EU)

ITSEC	Information Technology Security Evaluation Criteria
ITCEM	Information Security Technology Evaluation Manual

Canada

CTCPEC	Canadian Trusted Computer Product Evaluation Criteria

USA

FIPS 140-1	Validation of Cryptographic modules
TCSEC	Trusted Computer Security Evaluation Criteria

Others

XOPEN	Baseline Security Services
ECMA	COFC - Commercially Oriented Functional Class for Security Evaluation ECMA-Standard 205
	E-COFC – Extended Commercially Oriented Functional Class for Security Evaluation ECMA-Standard 271

Definitions

TBD

Acronyms and Abbreviations

TBD

Alternatives

Currently there are several alternative methods to demonstrate that a product meets the security and further quality requirements:

Manufacturer's Test Laboratory

The manufacturer of a product is using a comprehensive test plan to conduct a variety of highly complex and lengthy tests and evaluations. This comprises the development tests through manufacturing verification and field tests. As part of the comprehensive test plan the manufacturer includes all standards and test specification his product is complying to.
For all steps of development, production, and shipment process the manufacturer invests a significant amount of effort and time on quality assurance and development and production monitoring to guarantee a continuous level of quality and conformance to standards.

As an alternative the manufacturer has the option to get parts of his manufacturers test laboratory accredited by an accreditation body, if there is a market requirement.

The results obtained from all tests and evaluations will be documented in a test report. This detailed information will serve as a prove that the manufacturer's product meets the specified security functionality and further quality requirements. Additional factors which will certainly increase the trust are:

- the reputation which the manufacturer enjoy on the market
- the behaviour of the a product in the market
- liability of the manufacturer or supplier for hidden bugs.

The consumer trusts the declaration of the manufacturer or supplier of a it security product. By holding the manufacturer or supplier accountable is the best way to motivate them to ensure that his product meets and maintain the specified level of security and quality.
Advance IT products are subject to continuous testing and evaluation to clearly specified technical requirements during the complete development and manufacturing process. This requires a high degree of skill and in-depth knowledge of new technologies and design methodologies which makes it difficult, time consuming and quite costly and indeed unnecessary for third parties to repeat these tests and evaluations. In addition it provides the flexibility for the manufacturer to keep pace with product modifications and allows for fast response in a highly competitive market environment.

Evaluation by the Customer

If a SDoC is not sufficient for a consumer he has than the option either evaluate the efficiency and reliability of a product by himself or by calling on a consultant. This method is very reliable but extreme costly and requires adequate skill. Eventually the result is used by a small user group only.

Accredited Third Party Evaluation

If there are particular market needs or regulations which require a high degree of trustworthiness in the quality of a product than the manufacturer has the option to involve a trusted third party. This is normally a test house which is accredited by an accreditation body in accordance with ISO/IEC Guide 25 or EN 45001 and security related evaluation modules to prove the technical/organisational competence . The test house evaluates a product according evaluation criteria or regulations and produces a test report with his findings. The method ensures that the evaluation was impartial, competent, and the results are repeatable anytime. In addition the test results could be validated by an also accredited certification laboratory (EN 45011)
The certification laboratory will than certifies by means of a certificate that the product meets the security and further quality requirements.

Some regulation, i.e. the German Digital Signature Act, require mandatory certification of a IT product before it is put on the market. Mandatory basically means that the product underwent an extensive product test and the development and manufacturing process was assured by an independent test house.
Finally, which proof of trustworthiness a consumer wants depends heavily on the cost and benefits.

Each of the above method has its merits. Therefore, considering the Manufacturer's Test Laboratory and a SDoC is a valid and equal alternative to any certification process.

Recommendation for Use of a Suppliers' Declaration of Conformity

Procedure

The supplier confirms the compliance of a product with the applied evaluation criteria by issuing a SDoC in the same language as the technical operating instruction.
He keeps a file with the exact technical specification, construction data, test- and evaluation plan and results.
The SDoC is included to every product shipped and part of the operating instruction or any other customer documents.

Content

- Gives the name and address of the supplier who issued the declaration
- Describes the equipment and/or software in terms of name, type and model number
- Bears the place and date when the declartion was issued
- States the number and titles of the applied evaluation criteria, standards, design and assurance methodology, EU directives or if necessary company intern measures which ensure the compliance of the product with the required level of security and a date, if applicable
- Gives the evaluation report
- In case the evaluation was carried out by an independent test house, gives the name and address of the test laboratory which issued an evaluation report including a number and issue date
- Carries a legal binding signature of a supplier or his authorised representative.

The declaration of conformity is based on the requirements given in ISO/IEC Guide 22: Information on Manufacturer's Declaration of Conformity with standards or other technical specification

Evaluation Criteria

Below you will find a listing of available evaluation criteria for IT products:

ISO 15408-1, -2, -3	Evaluation Criteria for IT Security
	Protection Profiles based on ISO 15408
ISO 12119	Information Technology Software Products – Quality requirements and evaluation criteria
ISO/IEC 15504	Software Process Assessment (SPICE)
ISO/IEC WD 15939	Software Measurement Process Framework
ISO/IEC 9646	Conformance testing methodology and framework
ISO/IEC 14598	Software product evaluation

ITSEC	Information Technology Security Evaluation Criteria
ITCEM	Information Security Technology Evaluation Manual
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
FIPS 140-1	Validation of Cryptographic modules
TCSEC	Trusted Computer Security Evaluation Criteria
XOPEN	Baseline Security Services
ECMA	COFC - Commercially Oriented Functional Class for Security Evaluation ECMA-Standard 205
	E-COFC – Extended Commercially Oriented Functional Class for Security Evaluation ECMA-Standard 271

For further details, details refer to ISO/IEC WD 15443 A Framework for IT security assurance.

Annex A

Declaration of conformity of product security attributes

This annex A contains a set templates for security-declarations of an Transactional Smartcard Reader. This is intended as examples to help in the application of this Technical Report.
Alternative media (electronic files, electronic transfer, other) and identification technologies (bar-codes, ID units, other) may be used for automated transfer and exchange of the data in these declarations.

Annex A.1

Declaration of conformance of product security functional and assurance requirements for a Transactional Smartcard Reader

Supplier's Name :
Supplier's Address:

declares, under his sole responsibility, that the product

Product Name:
Product Type:
Model Number:
Seller/Manufacturer:
Weight: .... kg
Dimension: .... cm x .....cm x ....cm

based on test results obtained from test laboratories on sample testing for above product, that it

conforms to the following laws, standards, regulations and directives:

- 89/336/EEC	**CE**-mark	(EMC-Directive)
- 73/23/EEC		(LVD-Directive, CB-Report:UL 1765...)
- EN 50082-1		(EMC)
- EN 55022:1987, Class A		('radio disturbance')
- ISO 11469		(marking of plastic parts)
- IEC 950		(Product Safety)
- ISO 9001, 9002		(Certification of development and manufacturing)
-ISO 9241		(Human engineering)
-etc		

conforms to the following voluntary security functional and assurance requirements
ISO 15408-1, -2, -3 Evaluation Criteria for IT Security
PP/ 9902 Transactional Smartcard Reader Protection Profile
For details, refer to http://www.scssi.gouv.fr/present/si/ccsti/pp.html

Security Functional Requirements

Security requirements	Written evidence
FMT_MTD.1, FMT_SMR.1, FIA_UID.1, FPT_PHP.3	Management of TSF data and security roles ensure protection of keys during their management. Timing of identification is a dependency of security roles. Resistance to physical attacks contribute to protect keys.
FMT_MTD.1, FMT_SMR.1, FIA_UID.1, FPT_ITT.1	Management of TSF data and security roles ensure protection of cryptographic resources during their management. Timing of identification is a dependency of security roles. Basic internal TSF data transfer contributes to protect alteration of cryptographic resources.
FPT_PHP.3	Resistance to physical attacks contribute to protect keys in the TOE.
FCS_COP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FDP_DAU.1	Basic data authentication achieves firmware authentication. Cryptographic operations contribute to provide authentication.
FCS_COP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FIA_UAU.2, FIA_UID.1	User authentication before any action achieve authentication of the application software and related data. Cryptographic operations contribute to provide authentication. Timing of identification is a dependency of user authentication.
FPT_PHP.3	Resistance to physical attacks contribute to protect the TOE.
FDP_DAU.1, FIA_AFL.1, FIA_UAU.2, FIA_UID.1, FPT_PHP.3	Basic data authentication and User authentication prevent modification of internal TOE's assets. Authentication failure handling and Resistance to physical attacks contribute to protect keys in the TOE. Timing of identification is a dependency of user authentication.
FMT_MOF.1	Management of security functions behaviour ensure the continued correct operation of the TOE.
FCS_COP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FIA_UID.1, FMT_MTD.1, FMT_SMR.1	Evidence of distinguish identity is provided using cryptographic operation. Security roles and Management of TSF data contribute to manage this evidence.
FCS_COP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FIA_UID.1, FMT_MTD.1, FMT_SMR.1	Cryptographic operations contribute to provide authentication of the operator. Security roles and Management of TSF data contribute to manage this evidence. Timing of identification is a dependency of security roles.
FPT_FLS.1, FPT_RCV.2, FPT_TST.1	Failure with preservation of secure state, automated recovery and TSF testing ensure the TOE protection against internal technical failures.

Security Assurance Requirements

Evaluation Assurance Level
EAL4 Methodically designed, tested and reviewed Assurance level
Assurance Augmentations
ADV_IMP.2 Implementation of the TSF Higher hierarchical component
AVA_VLA.3 Relatively resistant Higher hierarchical

conforms to the following voluntary environmental program requirements
EPA Energy Star (saving electrical energy)

conforms to the environmental specifications, as listed in the ECO declaration below:

Operational data:

Energy consumption:

sleep mode:	.....	W
OFF mode:	.....	W

Physical emission:

Acoustical noise according to ISO 7779 and ISO 9296

declared **sound** power level			**sound** pressure level	
operational mode:	.....	bel	operational mode	..... dB(A)
sleep mode:	.....	bel	sleep mode	..... dB(A)

Materials:

The above described product does not contain:

- asbestos;
- cadmium (in plastic materials, packaging and inks);
- CFC and/or HCFC;
- chloroparaffins with chain length 10-13 C atoms, chlorination greater than 50% contained in mechanical plastic parts heavier than 25 g;
- lead contained in mechanical plastic parts heavier than 25g;
- mercury;
- PCB or PCT;
- polybrominated biphenyls, their oxides and their ethers contained in mechanical plastic parts heavier than 25 g.
- in concentrations exceeding the natural background levels.

Upgradability/Extendibility:

above system is upgradable in the following manner:

- upgrade possibilities (e.g. memory, fonts, etc.) ……..
- spare parts and service period …….. years

After end of life, this system can be given back to the supplier for environmental conscious recycling or disposal.
Please contact your "name of company" for take back information

Packaging:

- Packaging materials consist of: (describe and percentage by weight)
- ……
- Plastic packaging materials are marked according to ISO 11469
- Packaging recycling options such as participation in local collection and recycling consortiums are given

Above system contains following parts, which contain regulated materials and should be disposed of in an environmental acceptable manner.

.....

Issue Date: Signed by: